Auditoría de Seguridad: Vulnerabilidades Críticas en el Sistema de Autenticación y Gestión de Credenciales.

1 Resumen técnico

Durante la revisión de seguridad del portal administrativo interno, se identificaron múltiples vulnerabilidades que, en conjunto, representan un riesgo crítico para la organización. La falta de mecanismos de seguridad robustos en la autenticación, el almacenamiento y la gestión de contraseñas podría permitir el acceso no autorizado a datos sensibles de clientes y a áreas administrativas de alta criticidad. El sistema es vulnerable a ataques de fuerza bruta y a la filtración masiva de credenciales en caso de una brecha en la base de datos.

2 Tabla de Hallazgos

Hallazgo	Impacto	Recomendación técnica
Sin límite de intentos en login	Ataques de fuerza bruta	Implementar bloqueo progresivo por IP
Sin autenticación MFA	Acceso fácil si credenciales son robadas	Habilitar MFA obligatorio para administradores
Contraseñas en texto plano	Acceso total si la base de datos es comprometida	Hashear contraseñas con bcrypt o Argon2
Sin política de contraseña segura	Aumenta riesgo de contraseñas débiles	Aplicar políticas de longitud y caducidad

3 Redacción completa del hallazgo: Contraseñas en texto plano

3.1. Descripción del Hallazgo Se ha identificado que las contraseñas de los usuarios son almacenadas en texto plano en la base de datos de la aplicación. Esto significa que no se utiliza ningún algoritmo de *hashing* para proteger las credenciales, lo que las deja expuestas y legibles para cualquier persona con acceso a la base de datos.

3.2. Evidencia Técnica y Método de Prueba La vulnerabilidad fue confirmada mediante el acceso a una copia de la base de datos de desarrollo. Se consultó la tabla de usuarios y se

observó que la columna contraseña o similar contenía las credenciales en un formato de texto legible, sin ninguna transformación criptográfica.

3.3. Impacto Potencial Si un atacante logra comprometer la base de datos a través de una inyección SQL o cualquier otra técnica, todas las contraseñas de los usuarios quedarían expuestas de forma inmediata. Un atacante podría obtener control total de las cuentas, acceder a información confidencial de clientes, realizar acciones fraudulentas y comprometer la seguridad de todo el portal administrativo. Este riesgo es aún mayor si los usuarios reutilizan contraseñas en otros servicios.

3.4. Recomendación Técnica Detallada Se debe priorizar la implementación de un sistema de *hashing* criptográfico de contraseñas de manera inmediata. Se recomienda utilizar algoritmos de *hashing* fuertes y resistentes a ataques de fuerza bruta, como **bcrypt** o **Argon2**.

Los pasos para seguir son:

1. **Selección del Algoritmo:** Elegir un algoritmo de *hashing* como bcrypt o Argon2, que son conocidos por su resistencia y la inclusión de un factor de trabajo (work factor) que ralentiza el proceso de *hashing*, haciendo los ataques de fuerza bruta computacionalmente inviables.
2. **Uso de *Salts*:** Utilizar un *salt* (cadena de datos aleatoria) único y aleatorio para cada contraseña antes de aplicar el *hashing*. Esto previene los ataques de tabla arcoíris.
3. **Migración de Contraseñas:** En el proceso de migración, se deben forzar a los usuarios a cambiar sus contraseñas. A medida que un usuario inicia sesión, la contraseña en texto plano se *hashea* y se actualiza en la base de datos. Las credenciales antiguas y no *hasheadas* deben ser eliminadas de forma segura.